

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

The property located at 500 W Bradley Rd., Apartment
301B, Fox Point, WI 53217. See Attachment A.Case No. **19-M-114 (DEJ)**

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Wisconsin:

The property located at 500 W Bradley Rd., Apartment 301B, Fox Point, WI 53217. See Attachment A.

I find that the affidavit(s) or any recorded testimony, establish probable cause to search and seize the person or property described above and that such search will reveal:

See Attachment B.

YOU ARE COMMANDED to execute this warrant ON OR BEFORE June 12, 2019 (not to exceed 14 days)
☒ in the daytime between 6:00 a.m. and 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. David E. Jones,
(United States Magistrate Judge)☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____.Date and time issued: May 30, 2019 1:33 p.m.

Judge's signature

City and State: Milwaukee, Wisconsin

Case 2:19-mj-00114-DEJ Filed 06/06/19 Page 1 of 8 Document 2

Hon. David E. Jones

Printed Name and Title

U.S. Magistrate Judge

Return

Case No: 19-M-114 (DEJ)	Date and time warrant executed: 6/4/19 6AM	Copy of warrant and inventory left with: Luke Koltun & Kenneth Koltun
----------------------------	---	--

Inventory made in the presence of:

SA Jonathan Holmes, FBI

Inventory of the property taken and/or name of any person(s) seized:

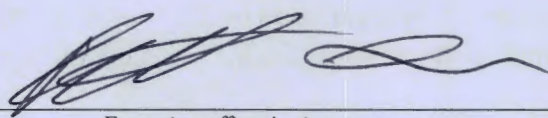
- 1.) White home built Gaming PC Next Case S/N 01172960800140
- 2.) Silver iPad S/n FGNNM03MFCM8
- 3.) Black Samsung Galaxy S9+ IMEI #353522095544785
- 4.) Dell Dimension E520 Desktop (white) Service Tag # 15QMQC1
- 5.) Yubico Encryption Key (Black) # 9 190 938
- 6.) Infinitive 32 GB USB (Black) S/N BM180426668B
- 7.) Black Lenovo Tablet S/N HA08MQ8E(14)
- 8.) HP Pavilion x360 Model 14m-cd 0001dx/SN 8CG907700C

BL

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the undersigned judge.

Date: 6/6/19


 Executing officer's signature

 Brett Lerner, Special Agent
 Printed name and title

Subscribed, sworn to, and returned before me this date:

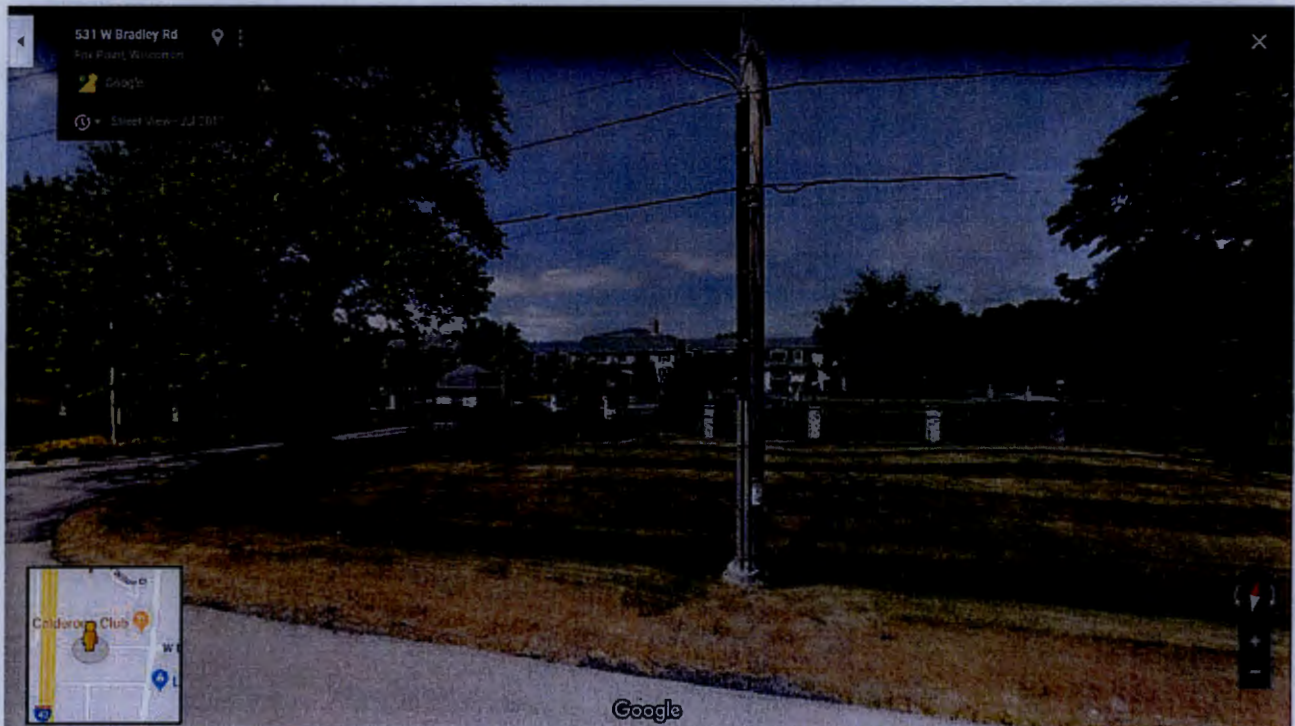
Date: June 6, 2019


 United States Magistrate Judge

ATTACHMENT A

Property to be searched

The property to be searched is 500 W Bradley Rd., Apartment 301B, Fox Point, WI 53217, as shown below:



ATTACHMENT B

Property to be seized

1. All records relating to violations of 18 U.S.C. § 1030(a)(5)(A) (unauthorized impairment of a protected computer), 1343 (wire fraud), and 371 (conspiracy to violate federal law), those violations involving Luke Koltun and occurring after October 18, 2016, including:
 - a. Records and information relating to the development, administration, and operation of booter.ninja;
 - b. Records and information relating to stresser/booter services and tools;
 - c. Records and information relating to website development, administration, and operation;
 - d. Records and information relating to the identity or location of the Luke Koltun and accomplices involved in booter/stresser services, including booter.ninja;
 - e. Bank account records, loan documents, wire transfer records, money order receipts, postal express mail envelopes, bank statements, safe deposit box keys and records, money containers, financial records or notes showing payment, receipt, concealment, transfer, or movement of money generated from booter.ninja or other booter/stresser services, or financial

transactions related to such activities, including any virtual or crypto currency;

f. Records of off-site storage locations including but not limited to safe deposit box keys and records, and records and receipts and rental agreements for storage facilities;

g. Records and information showing occupancy.

2. Computers or storage media used as a means to commit the violations described above.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

4. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the execution of the search of the premises described in Attachment A, law enforcement personnel are authorized to press the fingers (including thumbs) of individuals found at the premises to the Touch ID sensor of Apple brand device(s), such as an iPhone or iPad, found at the premises for the purpose of

attempting to unlock the device via Touch ID in order to search the contents as authorized by this warrant.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.